# Privacy Preserving Public Transport Ticketing Using Blockchain

Raphaël Rozenberg* - Supervised by: Konstantinos Markantonakis and Raja Naeem Akram

Information Security Group, Smart Card and IoT Security Center, RHUL
*École Normale Supérieure (ENS), PARIS

The Smart Card and Internet of Things Security Centre

## Objectives

- Propose and implement a privacy preserving token acquisition framework for cryptocurrencies that is more adapted to public transport ticketing and cheaper than existing coin mixers;
- Propose and implement a smart contract for decentralized and anonymous transport tickets.

## Introduction

Public transport is now going into its digital transformation. In this context, we wondered how blockchain technologies can contribute to a better ticketing system, not only for the user, but also for the transport operator and the environment. Indeed, public transport ticketing could benefit from the main features of blockchain: decentralisation, persistence and anonymity.

- As tickets will only become more digital, being able to pay for tickets with a cryptocurrency would be very welcomed by users who care about anonymity. However, current ways to do untraceable payments are expensive and not adapted to specific amounts. Our framework can be adapted to any classic cryptocurrency, but we chose to implement it on Ethereum.
- Paper tickets are currently in decline, due to their ecological cost. Contactless cards are now the most popular form of the new transport ticket. However, disputes can still happen between the client and the company. One way to resolve this problem would be to create a decentralised ticket on the blockchain, that would guarantee a certain number of properties that allow to avoid most disputes and preserve anonymity. This ticket would take the form of a smart contract.

## Untraceable payments

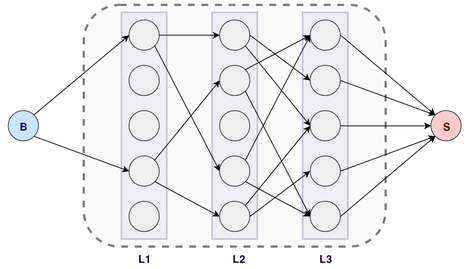



Figure 1: Layered structure

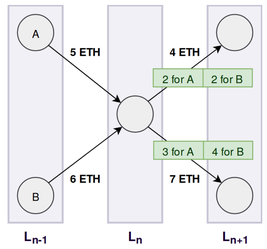



Figure 2: Transactions splittig and merging

This framework uses a network of nodes that split and merge the payments in order to make them untraceable. Contrary to traditional coin mixers, it does not require the users to put the same amount of money, which is restrictive in the context of transport ticketing (compared to money laundering for example).

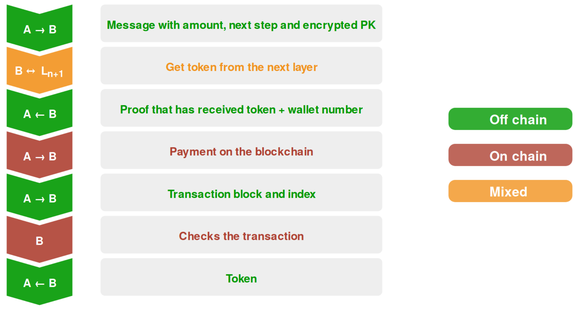
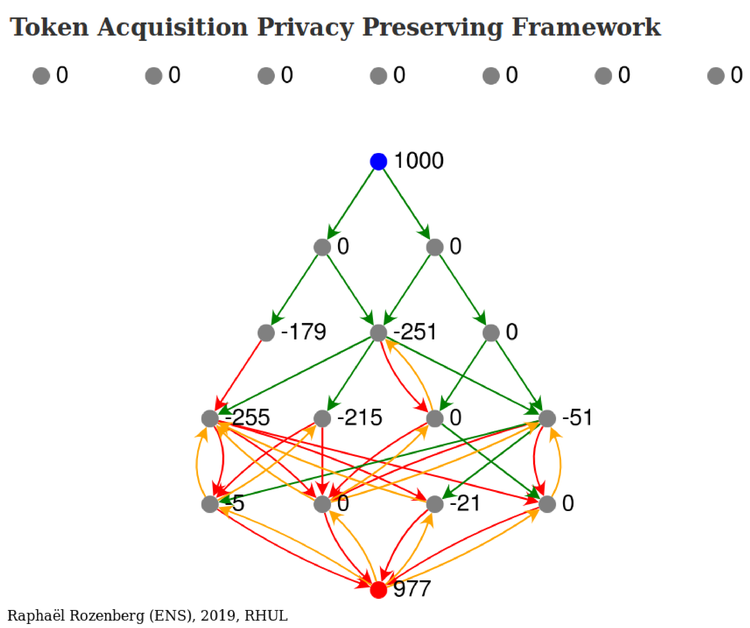
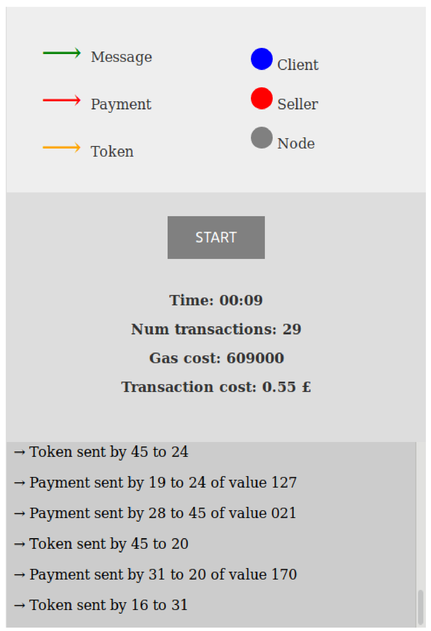



Figure 3: Exchange protocol between two nodes




## Smart contract ticket

The contract has an account system that associate each public key with a balance and some additional information. In order to avoid unnecessary payments, there is no actual transfer of Ether during normal use: the balances of the users are updated as part of the contract's state.
Properties that the contract verifies:

- **Proof of trip:** there can be a payment from an account to the transport operator only if the user has actually travelled the journey. For this, the user electronically signs at the gate a package containing the value of the journey as well as an encrypted description of the journey
- **Revocation:** users can withdraw their money at any time, but only unspent money.
- The transport operators cannot withdraw money from the contract, except if they refund all the users first and then kill the contract.

| Function | Cost |
|---|---|
| `constructor()` | 0.29 $ |
| `creditAccount()` | **0.01 $** |
| `payTravel()` | **0.02 $** |
| `askWithdraw()` + `withdrawFunds()` | 0.02 $ |
| `accessAccount()` | **0** |
| `beginKill()` + `endKill()` | 0.02 $ |

Table 1: Exchange rate: 216 $/ETH; gas price: 1 GWei/gas

## Contact Information

- Web: https://scc.rhul.ac.uk/
- Email: raphael.rozenberg@ens.fr